POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE PERSONAS FÍSICAS DE LA "AC FNMT USUARIOS"

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	06/04/2020
Revisado por:	FNMT-RCM	16/04/2020
Aprobado por:	FNMT-RCM	16/04/2020

HISTÓRICO DEL DOCUMENTO		
Versión	**Fecha**	**Descripción**
1.0	25/03/2014	Creación del documento
1.1	24/06/2016	Alineación con algunos requisitos del estándar ETSI 101 456
1.2	03/01/2017	Adaptación al estándar ETSI EN 319 412 - 2
1.3	22/12/2017	Revisión anual del documento. No se realizan cambios reseñables.
1.4	05/03/2019	Eliminación de prácticas de suspensión de certificados.
1.5	06/04/2020	Adaptación estructura RFC3647 e incorporación de medios de acreditación de la identidad

Referencia: DPC/CPUS0105/SGPSC/2020

Documento clasificado como: *Público*

ÍNDICES

ÍNDICE DE CONTENIDOS

1. INTRODUCCIÓN

1.1. OBJETO

1. El presente documento forma parte integrante de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC)* de la FNMT-RCM y tiene por objeto la información pública de las condiciones y características de los servicios de certificación y servicios de expedición de *Certificados* electrónicos por parte de la FNMT-RCM como *Prestador de Servicios de Confianza*, recogiendo las obligaciones y procedimientos que se compromete a cumplir en relación con el *Certificado de Persona Física* expedido por la AC FNMT Usuarios.

2. En especial deberá tenerse presente, a efectos interpretativos de estas *Política y prácticas de certificación Particulares*, el apartado "Definiciones" de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

3. Los *Certificados de usuarios* expedidos por la FNMT-RCM cuya *Política de Certificación y Prácticas de Certificación Particulares* se definen en el presente documento se consideran *Certificados Cualificados* de acuerdo con el Reglamento (UE) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, y conforme a la Ley 59/2003, de 19 de diciembre, de firma electrónica, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presta la FNMT – RCM.

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

4. La *Declaración de Prácticas de Certificación* de la FNMT-RCM como *Prestador de Servicios de Confianza* está estructurada, de un lado, por la parte común de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* (DGPC) de la FNMT-RCM, pues existen niveles de actuación análogos para todos los servicios de confianza de la Entidad y, de otro lado, por las *Políticas de Certificación y Prácticas de Certificación Particulares* aplicables a cada tipo de servicio de confianza que provee dicha Entidad.

5. De acuerdo con lo anterior, la estructura de la *Declaración de Prácticas de Certificación de la FNMT-RCM* es la siguiente:

   1) Por una parte, la ***Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica***, que debe considerarse cuerpo principal de la *Declaración de Prácticas de Certificación* en el que se describe, además de lo previsto en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, el régimen de responsabilidad aplicable a las partes involucradas en los servicios de confianza, los controles de seguridad aplicados a los procedimientos e instalaciones de la FNMT-RCM, en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de

sus bienes y activos, a la protección de datos de carácter personal y demás cuestiones de tipo informativo general que deben ponerse a disposición del público.

2) Y, por otra parte, la *Política de Certificación* específica en la que se describen las obligaciones y responsabilidades de las partes, los límites de uso de los *Certificados* y las ***Prácticas de Certificación Particulares*** que desarrollan los términos definidos en la política correspondiente y otorgan prestaciones adicionales o específicas sobre las generales establecidas en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

   La presente *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* (DPPP) concreta lo articulado en el cuerpo principal de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* y, por tanto, son parte integrante de ella, conformando, ambos, la *Declaración de Prácticas de Certificación* de la FNMT-RCM.

6. El presente documento define el conjunto de *Prácticas de Certificación* adoptadas por la FNMT-RCM como *Prestador de Servicios de Confianza* para la gestión del ciclo de vida de los *Certificados de Persona Física*,

   Nombre: Política de Certificación de *Certificados de Persona Física*

   Referencia / OID[1]: 1.3.6.1.4.1.5734.3.10.1.

   Tipo de política asociada: QCP-n. OID: 0.4.0.194112.1.0

   Versión: 1.5

   Fecha de expedición: 16/04/2020

   Localización: http://www.cert.fnmt.es/dpcs/

   DPC relacionada: Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM

   Localización: http://www.cert.fnmt.es/dpcs/

7. Las presentes Políticas de Certificación y Prácticas de Certificación Particulares de Certificados de Personas Físicas forman parte de la Declaración de Prácticas de Certificación y tendrán prelación sobre lo dispuesto en el cuerpo principal de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

8. Por tanto, en caso de que existiera contradicción entre el presente documento y lo dispuesto en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, tendrá preferencia lo aquí articulado.

[1] *Nota*: El OID o identificador de política es una referencia que se incluye en el *Certificado* al objeto de determinar un conjunto de reglas que indican la aplicabilidad de un determinado tipo de *Certificado* a la *Comunidad Electrónica* y/o clase de aplicación con requisitos de seguridad comunes.

9. La FNMT-RCM pone así, a disposición de la *Comunidad Electrónica* y demás interesados, tanto el presente documento como el documento de *DGPC* de la FNMT-RCM en los que se detalla:

   1) Los términos y condiciones que regulan la utilización de los *Certificados* expedidos por la FNMT-RCM.
   2) La *Política de Certificación* aplicable a los *Certificados* expedidos por la FNMT-RCM.
   3) Los límites de uso para los *Certificados* expedidos bajo esta *Política de Certificación*.
   4) Las obligaciones, garantías y responsabilidades de las partes involucradas en la expedición y uso de los *Certificados*.
   5) Los períodos de conservación de la información recabada en el proceso de registro y de los eventos producidos en los sistemas del *Prestador de Servicios de Confianza* relacionados con la gestión del ciclo de vida de los *Certificados* expedidos bajo esta *Política de Certificación*.

1.3. PARTES INTERVINIENTES

10. Las partes que intervienen en la gestión y uso de los *Servicios de Confianza* descritos en la presente *DPPP* son las siguientes:

    1. Autoridad de Certificación
    2. Autoridad de Registro
    3. *Suscriptores* de los *Certificados*
    4. Partes que confían
    5. Otros participantes

1.3.1. Autoridad de Certificación

11. La FNMT-RCM es la *Autoridad de Certificación* que expide los *Certificados* electrónicos objeto de la presente *DPPP*. A estos efectos, existen las siguientes Autoridades de Certificación:

    a) Autoridad de Certificación raíz. Dicha Autoridad expide exclusivamente *Certificados* de Autoridades de Certificación subordinadas. El *Certificado* raíz de esta AC viene identificado por la siguiente información:

Tabla 1 – Certificado de la AC FNMT raíz

Sujeto	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Emisor	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES

Número de serie (hex)	5D:93:8D:30:67:36:C8:06:1D:1A:C7:54:84:69:07
Validez	No antes: 29 de octubre de 2008. No después: 1 de enero de 2030
Longitud clave pública	RSA 4.096 bits
Algoritmo de firma	RSA – SHA256
Identificador de clave	F7 7D C5 FD C4 E8 9A 1B 77 64 A7 F5 1D A0 CC BF 87 60 9A 6D

b) Autoridad de Certificación subordinada: expide los Certificados de entidad final objeto de la presente *DPPP*. El *Certificado* de dicha Autoridad viene identificado por la siguiente información:

Tabla 2 – Certificado de la AC subordinada

Sujeto	CN = AC FNMT Usuarios, OU = CERES, O = FNMT-RCM, C = ES
Emisor	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Número de serie (hex)	45 5f 3a e1 5c 21 cd ba 54 4f 82 aa 47 51 eb db
Validez	No antes: 28 de octubre de 2014 No después: 28 de octubre de 2029
Longitud clave pública	RSA 2048 bits
Algoritmo de firma	RSA – SHA256
Identificador de clave	60 12 93 CA 20 B0 9A 03 29 5D 19 62 56 C6 95 3F F9 EB A8 11 DB 8E 3C E1 40 41 3C 1B FF E9 A8 69

1.3.2. Autoridad de Registro

12. La Autoridad de Registro realiza las tareas de identificación del solicitante, titular de los certificados, así como la comprobación de la documentación acreditativa de las circunstancias que constan en los mismos, la validación y la aprobación de las solicitudes de emisión, revocación y, en su caso, la renovación de dichos Certificados.

13. Podrán actuar como entidades de registro de FNMT-RCM aquellas Oficinas de Registro designadas por la FNMT-RCM con las que ésta suscriba el correspondiente instrumento legal para cubrir dicha finalidad.

1.3.3. Suscriptores de los certificados

14. Los *Suscriptores* de los *Certificados de Firma Electrónica son las personas físicas* que mantienen bajo su uso exclusivo los *Datos de creación de firma* asociados a dichos *Certificados*.

1.3.4. Partes que confían

15. Las partes que confían son aquellas personas físicas o jurídicas, diferentes del *Suscriptor*, que reciben y / o usan *Certificados* expedidos por la FNMT-RCM y, como tales, les es de aplicación lo establecido por la presente *DPPP* cuando deciden confiar efectivamente en tales *Certificados*.

1.3.5. Otros participantes

16. No estipulado.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

17. Los *Certificados de Firma electrónica* a los que aplica esta *DPPP* son *Certificados Cualificados* conforme al Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93 (Reglamento eIDAS) y de conformidad con los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y, ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

18. El Certificado de Persona Física es la certificación electrónica expedida por la FNMT-RCM que vincula a un *Suscriptor* con unos *Datos de verificación de Firma* y confirma su identidad.

19. Los *Certificados de firma electrónica* emitidos bajo esta *Política de Certificación* son expedidos a personas físicas y se consideran válidos como sistemas de identificación y de firma electrónicas, de conformidad con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, basados en Certificados electrónicos cualificados que son admitidos en virtud de su inclusión en las listas de servicios de confianza (TSL, por sus siglas en inglés) conforme a las especificaciones técnicas recogidas en el Anexo de la Decisión de la Comisión 2009/767/CE, de 16 de octubre de 2009 (modificada por la Decisión de la Comisión 2010/425/UE , de 28 de julio de 2010), por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas, con arreglo a la Directiva 2006/123/CE, de 12 de diciembre de 2006, del

Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior. Estas listas de servicios de confianza contienen información relativa a los *Prestadores de Servicios de Confianza* que expiden *Certificados cualificados* al público supervisados en cada Estado miembro, entre los cuales se encuentra la FNMT–RCM.

1.4.2. Restricciones en el uso de los certificados

20. En cualquier caso, si una *Entidad usuaria* o un tercero desean confiar en la *Firma electrónica* realizada con uno de estos *Certificados*, sin acceder al *Servicio de información y consulta sobre el estado de validez de los certificados* expedidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas y Prácticas de Certificación Particulares*, y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

21. No se podrá emplear este tipo de *Certificados* para:

- Firmar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
- Firmar software o componentes.
- Generar *Sellos de tiempo* para procedimientos de *Fechado electrónico.*
- Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente, como serían a título enunciativo y no limitativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación

1.5. ADMINISTRACIÓN DE POLÍTICAS

1.5.1. Entidad responsable

22. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, con NIF Q2826004-J, es la Autoridad de Certificación que expide los *Certificados* a los que aplica esta *Declaración de Prácticas y Políticas de Certificación*.

1.5.2. Datos de contacto

23. La dirección de contacto de la FNMT-RCM como *Prestador de Servicios de Confianza* es la siguiente:

Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28071 – MADRID

E-mail: ceres@fnmt.es

Teléfono: 902 181 696

1.5.3. Responsables de adecuación de la DPC

24. La Dirección de la FNMT-RCM dispone, dentro de sus competencias, de capacidad para especificar, revisar y aprobar los procedimientos de revisión y mantenimiento, tanto para las *Prácticas de Certificación Particulares*, como para la *Política de Certificación* correspondiente.

1.5.4. Procedimiento de aprobación de la DPC

25. La FNMT – RCM, a través de su Comité de Gestión del *Prestador de Servicios de Confianza*, vela por el cumplimiento de las *Declaraciones de Políticas y Prácticas de Certificación*, las aprueba y realiza el pertinente proceso de revisión de las mismas, con una periodicidad anual.

1.6. DEFINICIONES Y ACRÓNIMOS

1.6.1. Definiciones

26. A los efectos de lo dispuesto en el presente documento, particularizando las definiciones de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* y únicamente cuando los términos comiencen con letra mayúscula y estén en cursiva, se entenderá por:

- *Certificado de Persona Física*: *Certificado cualificado de firma electrónica* expedido por la AC FNMT Usuarios a una persona física que actúa como *Suscriptor*. Este es un tipo específico de certificado expedido por la FNMT – RCM y, por tanto, estará sujeto a las condiciones establecidas en su *Política y prácticas de certificación particulares*.
- *Servicio de Confianza*: Un servicio electrónico que consiste en alguna de las siguientes actividades: la creación, verificación, validación, gestión y conservación de F*irmas Electrónicas*, sellos electrónicos, *Sellos de Tiempo*, documentos electrónicos, servicios de entrega electrónica, autenticación de sitios web y *Certificados Electrónicos*, incluidos los certificados de *Firma Electrónica* y de sello electrónico.
- *Suscriptor*: Persona física que suscribe los términos y condiciones de uso de un *Certificado*. En los *Certificados de Persona Física* expedidos bajo la presente *Política*, coincide con la persona del *Titular*.
- *Titular* (de un *Certificado*): Es la persona física, mayor de 18 años o menor emancipado, cuya identidad queda vinculada a los *Datos de verificación de firma* (*Clave Pública*) del *Certificado* expedido por el *Prestador de Servicios de Confianza*. Por tanto, la identidad del *Titular* se vincula a lo firmado electrónicamente utilizando los *Datos de creación de firma* (*Clave Privada*) asociados al *Certificado*.

1.6.2. Acrónimos

27. A los efectos de lo dispuesto en la presente DPPP, son de aplicación los siguientes acrónimos, cuyo significado es acorde con el estándar europeo ETSI EN 319 411 "Policy and security requirements for Trust Service Providers issuing certificates":

AC: Autoridad de Certificación

AR: Autoridad de Registro

ARL: Lista de Revocación de Autoridades de Certificación

CN: Common Name (Nombre común)

CRL: Lista de *Certificados* revocados

DN: Distinguished Name (Nombre distintivo)

DPC: Declaración de Prácticas de Certificación

DGPC: Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica

eIDAS: Reglamento 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

ETSI: European Telecommunications Standards Institute

HSM: Módulo de seguridad criptográfico (Hardware Security Module). Es un dispositivo de seguridad que genera y protege claves criptográficas.

LCP: Política de *Certificado* ligera (Lightweight Certificate Policy)

NCP: Política de *Certificado* Normalizado

NCP+: Política de *Certificado* Normalizado Extendida

OCSP: Protocolo de internet usado para obtener el estado de un *Certificado* en línea (Online Certificate Status Protocol)

OID: Identificador de Objeto (Object IDentifier)

PIN: Personal Identification Number (Número de identificación personal)

PKCS: Public Key Cryptography Standards (Estándares PKI desarrollados por RSA Laboratorios)

TLS/SSL: Protocolos que proporcionan cifrado de datos y autenticación entre aplicaciones y servidores (Transport Layer Security/Secure Socket Layer protocol).

UTC: Tiempo coordinado universal (Coordinated Universal Time).

2. PUBLICACIÓN Y REPOSITORIOS

2.1. REPOSITORIO

28. La FNMT-RCM, como *Prestador de Servicios de Confianza*, mantiene un repositorio de información pública, disponible en horario 24x7, todos los días del año, en la dirección:

https://www.sede.fnmt.gob.es/descargas

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

29. La información relativa a la expedición de *Certificados* electrónicos objeto de la presente *DPPP* está publicada en la siguiente dirección:

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

2.3. FRECUENCIA DE PUBLICACIÓN

30. Cualquier modificación en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* o en las *Políticas* y *Prácticas de Certificación Particulares* será publicada de forma inmediata en la URL de acceso a las mismas.

31. En cuanto a la frecuencia de publicación de CRL, se define en el apartado "4.9.7 Características adicionales. Frecuencia de publicación".

2.4. CONTROL DE ACCESO A LOS REPOSITORIOS

32. Todos los repositorios anteriormente citados son de acceso libre para la consulta y, en su caso, descarga de la información. Así mismo, la FNMT-RCM ha establecido controles para impedir que personas no autorizadas puedan añadir, modificar o borrar información incluida en sus repositorios y para proteger la autenticidad e integridad de dicha información.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. NOMBRES

33. La codificación de los *Certificados* sigue el estándar RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Todos los campos definidos en el perfil de los *Certificados* en las *Políticas de Certificación* y *Prácticas de Certificación Particulares,* excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

3.1.1. Tipos de nombres

34. Los *Certificados* electrónicos de entidad final objeto de la presente *DPPP* contienen un nombre distintivo (*DN*) en el campo Subject Name, que se compone según se describe en la información relativa al perfil del *Certificado*.

35. En el procedimiento de acreditación de la identidad, como paso previo a la expedición de un *Certificado de Firma Electrónica,* la FNMT-RCM, a través de la *Oficina de Registro,* constatará la verdadera identidad del *Suscriptor*.

3.1.2. Significado de los nombres

36. Todos los nombres distintivos (*DN*) del campo Subject Name son significativos. La descripción de los atributos asociados al *Suscriptor* del *Certificado* es legible por humanos (véase el apartado 7.1.4 Formato de nombres del presente documento).

37. El campo Common Name de los *Certificados de Firma Electrónica* define al *Suscriptor* al que se le ha expedido el *Certificado*.

3.1.3. Seudónimos

38. En cuanto a la identificación de los *Suscriptores* mediante el uso de los *Certificados* expedidos bajo la presente Política de Certificación, la FNMT – RCM no admite el uso de seudónimos.

3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

39. Se aplican los requisitos definidos por el estándar X.500 de referencia en la norma ISO/IEC 9594.

3.1.5. Unicidad de los nombres

40. El nombre distintivo (*DN*) asignado a los *Certificados* expedidos a un *Suscriptor*, bajo las presentes DPPP y dentro del dominio del *Prestador de Servicios de Confianza,* será único.

3.1.6. Reconocimiento y autenticación de marcas registradas

41. La FNMT–RCM no asume compromiso alguno sobre el uso de signos distintivos, registrados o no, en la emisión de los *Certificados* expedidos bajo la presente *Política de Certificación.* Solo se permite la solicitud de *Certificados* que incluyan signos distintivos cuyo derecho de uso sea propiedad del *Titular* o se encuentre debidamente autorizado. La FNMT–RCM no está obligada a verificar previamente la titularidad o registro de los signos distintivos antes de la emisión de los *Certificados,* aunque figuren en registros públicos.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

3.2.1. Métodos para probar la posesión de la clave privada

42. La FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares*, que son generadas bajo el exclusivo control del *Suscriptor.*

3.2.2. Autenticación de la identidad de la organización

43. Los *Certificados* expedidos bajo las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares* no incorporan información de relación del Suscriptor (siempre una persona física) con ninguna organización, por lo que no es de aplicación la validación de dicha información.

3.2.3. Autenticación de la identidad de la persona física solicitante

44. La FNMT-RCM, como *Prestador de Servicios de Confianza*, antes de expedir un *Certificado de Persona Física* identificará al *Solicitante* del mismo, bien mediante presencia física ante una persona con capacidad para realizar la acreditación con la participación de una *Oficina de Registro* con la que la FNMT- RCM tenga suscrito un acuerdo o a la que sea de aplicación de una norma o una resolución administrativa, bien mediante la utilización de un *Certificado de firma electrónica* que confirme la identidad de la persona física solicitante, o bien utilizando otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, de conformidad con el Reglamento eIDAS. En el caso de identificación a distancia mediante un *Certificado de firma electrónica,* la FNMT- RCM aceptará *Certificados* de persona física emitidos por dicha entidad y los C*ertificados* electrónicos incorporados al DNIe.

45. La FNMT-RCM desarrollará los controles oportunos para comprobar la veracidad de la información incluida en el *Certificado*.

3.2.3.1. Comprobación directa mediante presencia física

46. Los *Solicitantes* de *Certificados de Persona Física* deberán comparecer físicamente para formalizar el procedimiento de confirmación de identidad personal, presentándose ante una persona con capacidad para realizar la acreditación y la participación de una *Oficina de Registro* autorizada, con los siguientes medios de identificación: Ciudadanos españoles: DNI, Pasaporte u otros medios admitidos en derecho a efectos de identificación (en los que conste su número de DNI/NIF). Ciudadanos de la UE: Tarjeta de Identificación de Extranjeros, o Certificado de Registro de Ciudadano de la Unión (donde conste el NIE) y Pasaporte o documento de identidad de país de origen, o Documento oficial de concesión del NIF y Pasaporte o documento de identidad de país de origen. Extranjeros: Tarjeta de Identificación de Extranjeros (donde conste el NIE) o Documento oficial de concesión del NIF y Pasaporte. El encargado de acreditación verificará que los documentos aportados cumplen todos los requisitos para confirmar la identidad del *Solicitante*.

47. La personación del *Solicitante* no será indispensable si la firma en la solicitud de expedición de un *Certificado* ha sido legitimada en presencia notarial o si se emplea algunos de los métodos descritos en el siguiente apartado.

3.2.3.2. Comprobación utilizando medios de identificación electrónica

48. La FNMT-RCM expedirá el *Certificado de Firma Electrónica* sin necesidad de que el peticionario comparezca ante una Oficina de Registro si en el proceso de solicitud de dicho

Certificado, el *Solicitante* se identifica utilizando un *Certificado cualificado de firma electrónica* perteneciente a alguno de los siguientes tipos:

- Un *Certificado de Persona Física* expedido bajo la presente *Política*.
- Un *Certificado* electrónico de los incorporados al DNIe.

49. No obstante, solo se permitirá la solicitud telemática del *Certificado de Persona Física* mediante el uso de los certificados electrónicos relacionados en el apartado anterior si, en el momento de la solicitud, no se ha superado el plazo máximo establecido por la legislación vigente desde la personación e identificación física del Suscriptor.

3.2.3.3. Comprobación indirecta mediante medios de aseguramiento equivalente a la presencia física de conformidad con el Derecho nacional

50. La FNMT-RCM podrá expedir el *Certificado de Persona Física* sin necesidad de que el peticionario comparezca ante una *Oficina de Registro* mediante la identificación del Solicitante utilizando métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, de conformidad con el Reglamento eIDAS.

3.2.4. Información no verificada del Suscriptor

51. Toda la información incorporada al *Certificado* electrónico es verificada por la *Autoridad de Registro*.

3.2.5. Validación de la autorización

52. Una vez confirmada la identidad del *Solicitante* por la *Oficina de Registro*, esta procederá a validar los datos y a enviarlos a la FNMT-RCM, junto con el código de solicitud remitido al *Solicitante* por correo electrónico. Esta transmisión de información se realizará mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM. Los datos personales y su tratamiento, en su caso, quedarán sometidos a la legislación específica.

53. Previa a la emisión del *Certificado*, la FNMT_RCM establece controles adicionales, como por ejemplo confirmar que el solicitante no está inscrito como difunto en los registros que el Ministerio de Justicia comunica a esta Entidad para tal fin.

54. No se emitirán *Certificados* a menores de edad, salvo que ostenten y acrediten su cualidad de emancipados. La Oficina de Registro será la encargada de realizar las validaciones relativas a este punto.

3.2.6. Criterios de interoperación

55. No existen relaciones de interactividad con Autoridades de Certificación externas a FNMT-RCM.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES

56. Bajo las presentes *Políticas de Certificación*, la FNMT-RCM no contempla ningún proceso de regeneración de claves.

57. Las condiciones de autenticación de una petición de renovación se desarrollan en el apartado correspondiente al proceso de renovación de *Certificados* de este documento.

3.3.1. Renovación rutinaria

58. Bajo las presentes *Políticas de Certificación*, la FNMT-RCM no contempla ningún proceso de renovación rutinaria.

3.3.2. Renovación después de una revocación

59. Bajo las presentes *Políticas de Certificación*, la FNMT-RCM no contempla ningún proceso de renovación después de una revocación.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

60. Previa a la revocación efectiva de los *Certificados*, la Autoridad de Registro identificará de forma fehaciente al *Solicitante* de la *Revocación* para vincularle con los datos únicos del *Certificado* a revocar.

61. Las condiciones de autenticación de una petición de revocación se desarrollan en el apartado correspondiente al proceso de revocación de *Certificados* de este documento.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. SOLICITUD DE CERTIFICADOS

4.1.1. Quién puede solicitar un Certificado

62. El *Solicitante* de este tipo de *Certificados* solo puede ser una persona física, mayor de edad o menor que acredite su condición de emancipado, en posesión de su número de Documento Nacional de Identidad o Número de Identificación de Extranjeros.

4.1.2. Proceso de registro y responsabilidades

63. El interesado accede al sitio web del *Prestador de Servicios de Confianza* de la FNMT-RCM, a través de la dirección http://www.cert.fnmt.es, donde se mostrarán las instrucciones del proceso completo de obtención del *Certificado de Persona Física*. El Solicitante deberá introducir su número de DNI o NIE, su primer apellido y su dirección de correo electrónico en el punto de recogida de datos dispuesto para ello. Así mismo, el *Solicitante* manifestará su

voluntad de obtener un *Certificado de Persona Física* y dará su consentimiento para que la FNMT-RCM pueda realizar una consulta al Sistema de Verificación de Datos de Identidad.

64. Posteriormente se generan las *Claves Pública* y *Privada* (en un dispositivo criptográfico – Token o Tarjeta criptográfica - si el *Solicitante* dispone del mismo o en el navegador si no dispone de dicho dispositivo) que serán vinculadas al *Certificado* que se generará en una fase posterior, y la FNMT – RCM asigna a la solicitud un código único.

65. Con carácter previo el Solicitante deberá consultar las Declaraciones General y Particular de Prácticas de Certificación en la dirección http://www.ceres.fnmt.es/dpcs/ con las condiciones de uso y obligaciones para las partes.

66. Al realizar esta solicitud se envía a la FNMT-RCM la *Clave Pública* generada, junto con las correspondientes pruebas de posesión de la *Clave Privada*, para la posterior expedición del *Certificado*. El envío de la *Clave Pública* a la AC para la generación del *Certificado* se realiza mediante un formato estándar, PKCS#10 o SPKAC, y utilizando un canal seguro.

67. La FNMT-RCM, tras recibir esta información comprobará, mediante la *Clave Pública* del peticionario, la validez de la información de la solicitud, la posesión y correspondencia de la pareja de *Claves* criptográficas por parte del peticionario, así como el tamaño de las claves generadas.

68. Esta información no dará lugar a la generación de un *Certificado* por parte de la FNMT-RCM, en tanto que esta no reciba la confirmación, por parte de la Oficina de Registro, de la identificación del peticionario. No obstante lo anterior, se tendrá en cuenta la posibilidad de identificación electrónica del peticionario del *Certificado de Persona Física*, generándose, en su caso, dicho *Certificado* sin que sea necesario que el *Solicitante* se persone físicamente ante una Oficina de Registro para acreditar su identidad.

69. El procedimiento de solicitud del *Certificado de Persona Física* finaliza con el envío, por parte de la FNMT – RCM, de un correo electrónico a la dirección facilitada por el *Solicitante* donde se le indica el código de solicitud único asignado y se le informa de las siguientes fases del proceso de obtención del *Certificado*.

70. El apartado 9.8 “Responsabilidades” del presente documento establece las responsabilidades de las partes en este proceso.

4.2. PROCEDIMIENTO DE SOLICITUD DE CERTIFICADOS

4.2.1. Realización de las funciones de identificación y autenticación

71. Para los *Certificados de Firma Electrónica*, el *Solicitante* aportará los datos requeridos y acreditará su identidad personal. La FNMT-RCM, a través de la *Oficina de Registro,* constatará la verdadera identidad del *Suscriptor* y conservará la documentación que la acredite. FNMT-RCM admitirá, en todo caso, la función e informe que realice la *Oficina de Registro*.

72. Para la emisión de *Certificados de Firma Electrónica*, la FNMT-RCM podrá identificar al *Solicitante*, de forma alternativa a la comparecencia en la *Oficina de Registro*, mediante el uso de un *Certificado de Firma Electrónica cualificado* según se describe en el apartado

"3.2.3.2. *Comprobación indirecta mediante medios de aseguramiento equivalente a la presencia física de conformidad con el Derecho nacional"*

4.2.2. Aprobación o rechazo de la solicitud del certificado

73. En los *Certificados de Firma Electrónica,* una vez confirmadas la identidad del *Solicitante* por la *Oficina de Registro*, ésta procederá a validar los datos y a enviarlos firmados, junto con el código de solicitud recogido en la fase de solicitud.

74. La transmisión de información a la FNMT-RCM se realizará mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

75. La FNMT-RCM recabará de los *Solicitantes* aquella información recibida de la *Oficina de Registro*, que sea necesaria para la expedición de los *Certificados* y para la comprobación de la identidad, almacenando la información exigida por la legislación de firma electrónica durante el periodo de quince (15) años tratándola con la debida diligencia para el cumplimiento de la legislación nacional vigente en materia de protección de datos de carácter personal.

76. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

4.2.3. Tiempo en procesar la solicitud

77. La solicitud aprobada de los Certificados de Firma Electrónica es procesada automáticamente por el sistema, por lo que no hay establecido un tiempo para este proceso.

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. Acciones de la AC durante la emisión

78. Una vez recibidos en la FNMT-RCM los datos personales del *Solicitante*, así como su código de solicitud, y confirmada su identidad conforme al apartado anterior, se procederá a la expedición del *Certificado de Persona Física*.

79. La expedición de *Certificados de Persona Física* supone la generación de documentos electrónicos que confirman la identidad del *Titular,* así como su correspondencia con la *Clave Pública* asociada. La expedición de *Certificados de Persona Física* de la FNMT-RCM sólo puede realizarla ella misma, en su calidad de *Prestador de Servicios de Confianza*, no existiendo ninguna otra entidad u organismo con capacidad de expedición de los mismos.

80. La FNMT-RCM, por medio de su *Firma electrónica* o *Sello electrónico*, autentica los *Certificados de Persona Física* y confirma la identidad del *Titular*. Por otro lado, y con el fin de evitar la manipulación de la información contenida en los *Certificados*, la FNMT-RCM utilizará mecanismos criptográficos que doten de autenticidad e integridad al *Certificado*.

81. La FNMT-RCM, en ningún caso, incluirá en un *Certificado* información distinta de la aquí mostrada, ni circunstancias, atributos específicos de los *Suscriptores* o límites distintos a los previstos en la presente *Declaración de Prácticas de Certificación*.

82. En cualquier caso, la FNMT-RCM actuará eficazmente para:

- Comprobar que el *Solicitante* del *Certificado de Persona Física* utiliza la *Clave Privada* correspondiente a la *Clave Publica* vinculada a la identidad del *Titular* del mismo. Para ello, la FNMT-RCM comprobará la correspondencia entre la *Clave privada* y la *Clave pública*.
- Lograr que la información incluida en el *Certificado de Persona Física* se base en la información proporcionada por el *Solicitante*.
- No ignorar hechos notorios que puedan afectar a la fiabilidad del *Certificado de Persona Física.*
- Lograr que el *DN* (nombre distintivo) asignado en el *Certificado* sea único en toda la *Infraestructura de Clave Pública* de la FNMT-RCM.

83. La emisión de los *Certificados de Firma Electrónica* atenderá a:

1. Composición de la estructura de datos que conforman el *Certificado*

   Con los datos recogidos durante el proceso de solicitud del *Certificado*, se procede a componer el nombre distintivo (DN) conforme al estándar X.500, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.

2. Generación del *Certificado* conforme al Perfil del *Certificado* correspondiente

84. El formato de los *Certificados*, expedidos por la FNMT-RCM bajo la presente *Política de Certificación*, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados Cualificados*, puede consultarse en la página http://www.cert.fnmt.es/dpcs/

4.3.2. Notificación de la emisión

85. Una vez emitido el *Certificado de Firma Electrónica*, la FNMT-RCM informará al *Solicitante* sobre la disponibilidad de *Certificado* para su descarga

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Proceso de aceptación

86. En el proceso de solicitud del *Certificado*, el *Solicitante* acepta las condiciones de uso y expresa su voluntad de obtener el *Certificado*, como requisitos necesarios para la generación del mismo.

87. La FNMT-RCM pone a disposición exclusiva del *Titular* su *Certificado de Persona Física* para que proceda a su descarga en la página web http://www.cert.fnmt.es.

88. En este proceso guiado de descarga, se le pedirá al *Solicitante* que introduzca su número de DNI o NIE, el primer apellido, así como el correspondiente código de solicitud obtenido en dicho proceso. Este código de solicitud será empleado, como clave concertada, para la generación por parte del *Titular* de una firma electrónica de las condiciones de uso del *Certificado*, como requisito imprescindible para acceder a la descarga del mismo y como aceptación de dichas condiciones de uso, remitiéndolas firmadas a la FNMT – RCM. Si el

Certificado de Persona Física aún no hubiera sido generado por cualquier motivo, el proceso le informará de este hecho.

89. En el momento de la descarga del *Certificado de Persona Física*, este se instalará en el soporte en el que se generaron las *Claves* durante el proceso de solicitud (token criptográfico o, en su defecto, el *Navegador* desde el cual hizo la solicitud). En la citada página web de la FNMT-RCM se indican los *Navegadores* soportados y normas de instalación de los certificados.

4.4.2. Publicación del certificado por la AC

90. Los *Certificados* generados son almacenados en un repositorio seguro de la FNMT-RCM, con acceso restringido.

4.4.3. Notificación de la emisión a otras entidades

91. No se realizan notificaciones de emisión a otras entidades.

4.5. PAR DE CLAVES Y USO DEL CERTIFICADO

4.5.1. Clave privada y uso del certificado

92. La FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo la presente *Política de Certificación*. Corresponde la condición de custodio, *Suscriptor* y responsable sobre el control de las claves del *Certificado*, al *Titular* del *Certificado*.

93. Los *Certificados de Firma Electrónica* emitidos bajo esta *Política de Certificación* son certificados cualificados expedidos a personas físicas y se consideran válidos como sistemas de identificación y de firma electrónicas, de conformidad con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

4.5.2. Uso del certificado y la clave pública por terceros que confían

94. Los terceros que confían en las *Firmas electrónicas* realizadas con las *Claves privadas* asociadas al *Certificado* se atendrán a las obligaciones y responsabilidades definidas en la presente *DPPP*.

4.6. RENOVACIÓN DEL CERTIFICADO

95. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.1. Circunstancias para la renovación del certificado

96. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.2. Quién puede solicitar la renovación del certificado

97. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.3. Procesamiento de solicitudes de renovación del certificado

98. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.4. Notificación de la renovación del certificado

99. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.5. Conducta que constituye la aceptación de la renovación del certificado

100. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.6. Publicación del certificado renovado

101. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.7. Notificación de la renovación del certificado a otras entidades

102. Bajo las presentes Políticas de Certificación, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.6.8. Procesamiento de solicitudes de modificación del certificado

103. No se estipula la modificación.

4.7. RENOVACIÓN CON REGENERACIÓN DE LAS CLAVES DEL CERTIFICADO

104. Bajo las presentes Políticas de Certificación, la renovación con regeneración de claves de los *Certificados* se realiza siempre emitiendo nuevas claves, siguiendo el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

105. Solo se permitirá una única renovación del *Certificado de Persona Física*. El *Titular* que ya hubiera realizado una renovación de su *Certificado* y quisiera seguir utilizando un *Certificado de Persona Física* bajo las presentes *Políticas de Certificación y Prácticas de Certificación*

Particulares, deberá solicitar un nuevo *Certificado* y confirmar su identidad conforme al procedimiento descrito en el apartado "Comprobación de la identidad mediante comparecencia física" de este documento.

106. Podrán solicitar la renovación de los *Certificados de Persona Física* expedidos por la FNMT-RCM los *Titulares* de los mismos, siempre que en el momento de la solicitud tengan un *Certificado* en vigor y sus *Datos de creación de Firma* asociados, y dicha solicitud se efectúe durante los sesenta (60) días anteriores a su c*aducidad*.

107. La renovación de un *Certificado de Persona Física* consistirá en la generación de nuevos *Datos de verificación de Firma* y de *creación de Firma*, así como en la expedición de un nuevo *Certificado de Persona Física*. La solicitud de renovación se hará a través de la dirección http://www.ceres.fnmt.es.

108. El *Certificado* que está próximo a caducar seguirá siendo válido hasta que expire el período de vigencia del mismo. En caso de solicitarse la revocación del *Certificado de Persona Física* durante el período de tiempo en el que el *Titular* posee dos *Certificados* activos, la FNMT-RCM procederá a revocar ambos *Certificados*.

109. El procedimiento establecido para la renovación de un *Certificado de Persona Física* no requiere la personación del peticionario, ya que se le identificará telemáticamente mediante la utilización de sus *Datos de creación de Firma*. Tanto el proceso de la solicitud como la obtención del *Certificado* se realizarán de forma telemática, requiriéndose en todo caso la generación por parte del peticionario de una *Firma electrónica avanzada*, realizada con un *Certificado electrónico cualificado*, del documento de solicitud de renovación. No obstante, solo se permitirá la renovación telemática del *Certificado de Persona Física* cuando no se haya superado el plazo máximo de 5 años desde la personación e identificación física del *Titular* que establece el artículo 13.4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

110. Las funcionalidades del DNIe se tendrán en cuenta a los efectos de identificación de acuerdo con su legislación específica.

111. La utilización de los *Certificados de Persona Física* renovados se sujeta a las mismas condiciones generales y particulares vigentes en cada momento y establecidas para este tipo de *Certificados* en su correspondiente *Declaración de Practicas de Certificación*.

4.7.1. Circunstancias para la renovación con regeneración de claves

112. Las claves de los *Certificados* se renovarán por caducidad próxima de las actuales claves, a petición del solicitante de la renovación.

4.7.2. Quién puede solicitar la renovación con regeneración de claves

113. Se seguirá el mismo proceso que el descrito para la emisión de un Certificado nuevo.

4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves

114. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.4. Notificación de la renovación con regeneración de claves

115. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.5. Conducta que constituye la aceptación de la renovación con regeneración de claves

116. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.6. Publicación del certificado renovado

117. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.7. Notificación de la renovación con regeneración de claves a otras entidades

118. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo

4.8. MODIFICACIÓN DEL CERTIFICADO

119. No es posible realizar modificaciones de los *Certificados* expedidos. Por tanto, cualquier necesidad de modificación conlleva la expedición de un nuevo *Certificado*.

4.8.1. Circunstancias para la modificación del certificado

120. No se estipula la modificación.

4.8.2. Quién puede solicitar la modificación del certificado

121. No se estipula la modificación.

4.8.3. Procesamiento de solicitudes de modificación del certificado

122. No se estipula la modificación.

4.8.4. Notificación de la modificación del certificado

123. No se estipula la modificación.

4.8.5. Conducta que constituye la aceptación de la modificación del certificado

124. No se estipula la modificación.

4.8.6. Publicación del certificado modificado

125. No se estipula la modificación.

4.8.7. Notificación de la modificación del certificado a otras entidades

126. No se estipula la modificación.

4.9. REVOCACIÓN DEL CERTIFICADO

127. Los *Certificados de Persona Física* expedidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

a) Terminación del período de validez del *Certificado*.

b) Cese en la actividad como *Prestador de Servicios de Confianza* de la FNMT-RCM, salvo que, previo consentimiento expreso del *Suscriptor*, los *Certificados* expedidos por la FNMT-RCM hayan sido transferidos a otro *Prestador de Servicios de Confianza*.

En estos dos casos [a) y b)], la pérdida de eficacia de los *Certificados* tendrá lugar desde que estas circunstancias se produzcan.

c) Revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento.

128. Los efectos de la revocación del *Certificado*, esto es, la extinción de su vigencia, surtirán efecto desde la fecha en que la FNMT-RCM tenga conocimiento cierto de cualquiera de los hechos determinantes y desde el momento de hacerlo constar en su *Servicio de información y consulta sobre el estado de los certificados*.

129. A los efectos enumerados anteriormente, la expedición de un *Certificado de Persona Física* cuando exista otro vigente a favor del mismo *Titular*, conllevará la revocación inmediata del *Certificado* anterior. La única excepción a este caso se produce cuando la expedición de un *Certificado de Persona Física* sea causa de un proceso de renovación del mismo durante el periodo de tiempo de sesenta (60) días antes de su fecha de caducidad, en cuyo caso el *Certificado* que está próximo a caducar seguirá siendo válido hasta que expire el período de vigencia del mismo. Durante este tiempo, de producirse la revocación de dicho *Certificado* conforme al apartado siguiente, se producirá la extinción de la vigencia de ambos *Certificados.*

La FNMT-RCM pone a disposición de los *Suscriptores*, terceros que confían, proveedores de software y terceras partes una vía de comunicación a través de la sede electrónica de la FNMT-RCM: https://www.sede.fnmt.gob.es/

4.9.1. Circunstancias para la revocación

4.9.1.1. Circunstancias para la revocación del certificado del suscriptor

130. La solicitud de revocación de los *Certificados* podrá efectuarse durante el período de validez que consta en el *Certificado.*

131. Serán causas admitidas para la revocación de un *Certificado de Persona Física* las expuestas a continuación:

a) La solicitud de revocación por parte del *Suscriptor*. En todo caso deberá dar lugar a esta solicitud:

- La pérdida del soporte del *Certificado*.
- La utilización por un tercero de los *Datos de Creación de Firma*, correspondientes a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad personal del *Titular*.
- La violación o puesta en peligro del secreto de los *Datos de Creación de Firma* o de la clave privada asociada al *Certificado.*
- La no aceptación de las nuevas condiciones que puedan suponer la expedición de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

c) Fallecimiento o incapacidad sobrevenida, total o parcial, del *Titular*

d) Inexactitudes en los datos aportados por el *Solicitante* para la obtención del *Certificado*, o alteración de los datos aportados para la obtención del *Certificado* o modificación de las circunstancias verificadas para la expedición del *Certificado*, de manera que este ya no fuera conforme a la realidad.

e) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte del *Suscriptor* o del *Solicitante* del *Certificado* si, en este último caso, hubiese podido afectar al procedimiento de expedición del *Certificado*.

f) Violación o puesta en peligro del secreto de los *Datos de Creación de Firma*.

g) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte de una *Oficina de Registro* si hubiese podido afectar al procedimiento de expedición del *Certificado*.

h) Resolución del contrato suscrito entre el *Suscriptor* y la FNMT-RCM.

i) Cese en la actividad del *Prestador de Servicios de Confianza* salvo que la gestión de los *Certificados* electrónicos expedidos por aquél sea transferida a otro *Prestador de Servicios de Confianza*.

132. En ningún caso la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a f) del presente apartado, debiendo ser notificadas a esta entidad de forma fehaciente mediante entrega de los documentos e informaciones necesarias para verificarlo.

133. La FNMT-RCM únicamente será responsable de las consecuencias que se desprendan de no haber revocado un *Certificado* en los siguientes supuestos:

- Que la revocación se debiera haber efectuado por solicitud fehaciente por parte del *Suscriptor* o por medio de los sistemas puestos a disposición por la FNMT-RCM para este fin.
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.

- Que las causas c) a f) del presente apartado le sean acreditadas fehacientemente, previa identificación del *Suscriptor* y/o *Solicitante* de la revocación (o persona con facultades de representación suficientes, si se produjera incapacidad sobrevenida del *Suscriptor*).

134. La FNMT-RCM podrá revocar de oficio los *Certificados* de los *Suscriptores* cuando se den las causas b) a i) del presente apartado.

135. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos y/o *Certificado* y las inexactitudes sobre los datos o falta de diligencia en su comunicación a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

136. La revocación de los *Certificados* implica, además de su extinción y la imposibilidad de seguir utilizando los *Datos de creación de firma* o claves privadas asociados, la finalización de la relación y régimen de uso de dicho *Certificado* y su *Clave privada* con la FNMT-RCM.

4.9.1.2. Circunstancias para la revocación del certificado de la CA subordinada

137. Se atenderá a lo dispuesto en el "Plan de Actuación ante Compromiso de la Infraestructura de Clave Pública de FNMT-RCM"

4.9.2. Quién puede solicitar la revocación

138. La revocación de un *Certificado* solamente podrá ser solicitada por:

- la *Autoridad de Certificación* y la *Autoridad de Registro*
- el *Suscriptor* o persona autorizada, en la *Oficina de Registro* habilitada a tal efecto
- en su caso, el *Suscriptor,* a través del teléfono habilitado para tal fin (previa identificación del Solicitante) cuyo número se hace público en la web de la FNMT – RCM y que estará operativo en horario 24x7.

139. La FNMT-RCM podrá revocar de oficio los *Certificados* en los supuestos recogidos en la presente Declaración de Prácticas y Políticas de Certificación.

4.9.3. Procedimiento de solicitud de la revocación

140. La solicitud de revocación de los *Certificados de Persona Física* podrá efectuarse durante el período de validez que consta en el *Certificado*.

141. La revocación de un *Certificado de Persona Física* solamente podrá ser solicitada por el *Titular* o persona con facultades de representación suficientes, si se produjera incapacidad sobrevenida del *Titular*, en los términos recogidos en las presentes *Políticas de Certificación y Prácticas de Certificación Particulares*.

142. El proceso de revocación puede realizarse de forma ininterrumpida 24x7, a través del Servicio de Revocación telefónica puesto a disposición de los usuarios para esta finalidad, asegurando la revocación del *Certificado* en un plazo inferior a 24h.

143. Durante la revocación telefónica, el solicitante de la revocación tendrá que confirmar los datos que se le soliciten y aportar aquellos que sean imprescindibles para la validación de forma inequívoca de su capacidad para solicitar dicha revocación.

144. Si el *Titular* está en posesión del *Certificado de Persona Física* y sus *Datos de creación de Firma* asociados, es posible autenticar su identidad con base a dicho *Certificado*, por lo que se le permite solicitar la revocación del mismo a través de Internet, o de cualquier otra vía equivalente que permita la conexión a la dirección http://www.ceres.fnmt.es, siguiendo las instrucciones expuestas en dicho sitio web. Este servicio estará disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará esta última circunstancia en la dirección http://www.ceres.fnmt.es, si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

145. Adicionalmente, se puede solicitar la revocación de cualquier *Certificado* a través de una *Oficina de Registro*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica. El solicitante deberá presentarse en su *Oficina de Registro,* donde se acreditará su identidad, se validará su capacidad para revocar dicho *Certificado* y se consignará la causa de revocación. La Oficina enviará de forma telemática mediante la aplicación de registro los datos a la FNMT-RCM, y procederá a la revocación del *Certificado*.

146. Tan pronto la revocación sea efectiva, el *Suscriptor* y solicitante de la revocación serán notificados a través de la dirección de correo electrónico.

147. Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Certificados Revocados,* conteniendo el número de serie del *Certificado* revocado, así como la fecha, hora y causa de revocación. Una vez que un *Certificado* ha sido revocado, su vigencia queda definitivamente extinguida, sin posibilidad de revertir su estado.

4.9.4. Periodo de gracia de la solicitud de revocación

148. No existe periodo de gracia asociado a este proceso, pues la revocación se realiza de forma inmediata a la recepción verificada de la solicitud de revocación.

4.9.5. Plazo de tiempo para procesar la solicitud de revocación

149. La FNMT – RCM procede a la revocación inmediata del *Certificado* en el momento de verificar la identidad del *Solicitante* o, en su caso, de la veracidad de la solicitud realizada mediante resolución judicial o administrativa. En cualquier caso, la revocación efectiva del *Certificado* se realizará en menos de 24 horas desde la recepción de la solicitud de revocación.

4.9.6. Obligación de verificar las revocaciones por las partes que confían

150. Las terceras partes que confían y aceptan el uso de los *Certificados* emitidos por la FNMT – RCM están obligadas a verificar, por medio de uno de los mecanismos disponibles (Listas de Revocación CRL y/o OCSP), el estado de los *Certificados*:

- la *Firma Electrónica Avanzada* o el *Sello Electrónico Avanzado* del *Prestador de Servicios de Confianza* emisor del *Certificado,*

- que el *Certificado* continúa vigente y activo, y
- el estado de los *Certificados* incluidos en la *Cadena de Certificación.*

4.9.7. Frecuencia de generación de CRLs

151. Las *Listas de Revocación* (*CRL*) de los *Certificados de Firma Electrónica* se emiten al menos cada 12 horas, o cuando se produce una revocación y tienen un periodo de validez de 24 horas. Las *CRL* de los *Certificados* de *Autoridad* se emiten cada 6 meses, o cuando se produce una revocación de una *Autoridad de Certificación* subordinada y tienen un periodo de validez de 6 meses.

4.9.8. Periodo máximo de latencia de las CRLs

152. La publicación de las *Listas de Revocación* se realiza en el momento de generación de dichas Listas, por lo que el periodo de latencia entre la generación de la CRL y su publicación es nulo.

4.9.9. Disponibilidad del sistema de verificación online del estado de los certificados

153. La información relativa al estado de los *Certificados* estará disponible en línea las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema se pondrá en marcha el Plan de continuidad de negocio para solventar el incidente a la mayor brevedad posible.

4.9.10. Requisitos de comprobación en línea de la revocación

154. La comprobación en línea del estado de revocación de los *Certificados de Firma Electrónica* puede realizarse mediante el *Servicio de información del estado de los Certificados*, ofrecido a través de OCSP según se describe en el apartado 4.10 del presente documento. El interesado en utilizar dicho servicio deberá:

- Comprobar la dirección contenida en la extensión AIA (Authority Information Access) del *Certificado*.
- Comprobar que la respuesta OCSP está firmada / sellada.

4.9.11. Otras formas de aviso de revocación disponibles

155. No definidas.

4.9.12. Requisitos especiales de revocación de claves comprometidas

156. No existen requisitos especiales para el caso de revocación de *Certificados* causada por un compromiso de claves, siendo de aplicación lo descrito para el resto de las causas de revocación.

4.9.13. Circunstancias para la suspensión

157. No se contempla la suspensión de *Certificados*.

4.9.14. Quién puede solicitar la suspensión

158. No se contempla la suspensión de *Certificados*.

4.9.15. Procedimiento para la petición de la suspensión

159. No se contempla la suspensión de *Certificados*.

4.9.16. Límites sobre el periodo de suspensión

160. No se contempla la suspensión de *Certificados*.

4.10. SERVICIO DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

4.10.1. Características operativas

161. La información relativa a la validación de los *Certificados* electrónicos objeto de la presente *DPPP* es accesible a través de los medios descritos en la *DGPC*.

4.10.2. Disponibilidad del servicio

162. La FNMT-RCM garantiza el acceso a este servicio, en horario 24x7, por parte de los *Usuarios* y las partes que confían en los *Certificados*, de forma segura, rápida y gratuita.

4.10.3. Características opcionales

163. No estipuladas.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

164. La suscripción finalizará en el momento de extinción de la vigencia del *Certificado*, ya sea por expiración del periodo de vigencia o por revocación del mismo. De no llevarse a cabo la renovación del *Certificado* se considerará extinguida la relación entre el *Suscriptor* y la FNMT-RCM.

165. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado de Firma Electrónica* emitido por la FNMT-RCM cuando exista otro vigente a favor del mismo *Suscriptor,* y perteneciente a la misma *Ley de Emisión,* conllevará la revocación del primero obtenido.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Prácticas y políticas de custodia y recuperación de claves

166. La FNMT-RCM no recuperará las *Claves privadas* asociadas a los *Certificados*.

4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión

167. No estipulado.

5. CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTOS Y DE PERSONAL

168. Véase el apartado correspondiente en la DGPC.

5.1. CONTROLES DE SEGURIDAD FÍSICA

169. Véase el apartado correspondiente en la DGPC.

5.1.1. Ubicación de las instalaciones

170. Véase el apartado correspondiente en la DGPC.

5.1.2. Acceso Físico

171. Véase el apartado correspondiente en la DGPC.

5.1.3. Electricidad y Aire Acondicionado

172. Véase el apartado correspondiente en la DGPC.

5.1.4. Exposición al agua

173. Véase el apartado correspondiente en la DGPC.

5.1.5. Prevención y Protección contra incendios

174. Véase el apartado correspondiente en la DGPC.

5.1.6. Almacenamiento de Soportes

175. Véase el apartado correspondiente en la DGPC.

5.1.7. Eliminación de Residuos

176. Véase el apartado correspondiente en la DGPC.

5.1.8. Copias de Seguridad fuera de las instalaciones

177. Véase el apartado correspondiente en la DGPC.

5.2. CONTROLES DE PROCEDIMIENTO

178. Véase el apartado correspondiente en la DGPC.

5.2.1. Roles de Confianza

179. Véase el apartado correspondiente en la DGPC.

5.2.2. Número de personas por tarea

180. Véase el apartado correspondiente en la DGPC.

5.2.3. Identificación y autenticación para cada rol

181. Véase el apartado correspondiente en la DGPC.

5.2.4. Roles que requieren segregación de funciones

182. Véase el apartado correspondiente en la DGPC.

5.3. CONTROLES DE PERSONAL

183. Véase el apartado correspondiente en la DGPC.

5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos

184. Véase el apartado correspondiente en la DGPC

5.3.2. Procedimientos de verificación de antecedentes

185. Véase el apartado correspondiente en la DGPC

5.3.3. Requisitos de formación

186. Véase el apartado correspondiente en la DGPC

5.3.4. Requisitos y frecuencia de actuación formativa

187. Véase el apartado correspondiente en la DGPC

5.3.5. Secuencia y frecuencia de rotación laboral

188. Véase el apartado correspondiente en la DGPC

5.3.6. Sanciones por acciones no autorizadas

189. Véase el apartado correspondiente en la DGPC

5.3.7. Requisitos de contratación de personal

190. Véase el apartado correspondiente en la DGPC

5.3.8. Suministro de documentación al personal

191. Véase el apartado correspondiente en la DGPC

5.4. PROCEDIMIENTOS DE AUDITORÍA

192. Véase el apartado correspondiente en la DGPC.

5.4.1. Tipos de eventos registrados

193. Véase el apartado correspondiente en la DGPC.

5.4.2. Frecuencia de procesamiento de registros

194. Véase el apartado correspondiente en la DGPC.

5.4.3. Periodo de conservación de los registros

195. Véase el apartado correspondiente en la DGPC.

5.4.4. Protección de los registros

196. Véase el apartado correspondiente en la DGPC.

5.4.5. Procedimientos de copias de seguridad de los registros auditados

197. Véase el apartado correspondiente en la DGPC.

5.4.6. Sistemas de recolección de registros

198. Véase el apartado correspondiente en la DGPC.

5.4.7. Notificación al sujeto causante de los eventos

199. Véase el apartado correspondiente en la DGPC.

5.4.8. Análisis de vulnerabilidades

200. Véase el apartado correspondiente en la DGPC.

5.5. ARCHIVADO DE REGISTROS

201. Véase el apartado correspondiente en la DGPC.

5.5.1. Tipos de registros archivados

202. Véase el apartado correspondiente en la DGPC.

5.5.2. Periodo de retención del archivo

203. Véase el apartado correspondiente en la DGPC.

5.5.3. Protección del archivo

204. Véase el apartado correspondiente en la DGPC.

5.5.4. Procedimientos de copia de respaldo del archivo

205. Véase el apartado correspondiente en la DGPC.

5.5.5. Requisitos para el sellado de tiempo de los registros of Records

206. Véase el apartado correspondiente en la DGPC.

5.5.6. Sistema de archivo

207. Véase el apartado correspondiente en la DGPC.

5.5.7. Procedimientos para obtener y verificar la información archivada

208. Véase el apartado correspondiente en la DGPC.

5.6. CAMBIO DE CLAVES DE LA AC

209. Véase el apartado correspondiente en la DGPC.

5.7. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

210. Véase el apartado correspondiente en la DGPC.

5.7.1. Gestión de incidentes y vulnerabilidades

211. Véase el apartado correspondiente en la DGPC.

5.7.2. Actuación ante datos y software corruptos

212. Véase el apartado correspondiente en la DGPC.

5.7.3. Procedimiento ante compromiso de la clave privada de la AC

213. Véase el apartado correspondiente en la DGPC.

5.7.4. Continuidad de negocio después de un desastre

214. Véase el apartado correspondiente en la DGPC.

5.8. CESE DE LA ACTIVIDAD DEL PRESTADOR DE SERVICIOS DE CONFIANZA

215. Véase el apartado correspondiente en la DGPC.

6. CONTROLES DE SEGURIDAD TÉCNICA

216. Véase el apartado correspondiente en la *DGPC*.

6.1. GENERACIÓN E INSTALACIÓN DE LAS CLAVES

6.1.1. Generación del par de claves

6.1.1.1. Generación del par de Claves de la CA

217. En relación con la generación de las *Claves* de AC que la FNMT-RCM necesita para el desarrollo de su actividad como *Prestador de Servicios de Confianza,* véase el apartado correspondiente en la *DGPC*.

6.1.1.2. Generación del par de Claves de la RA

218. No estipulado

6.1.1.3. Generación del par de Claves de los Suscriptores

219. En relación con la generación de las *Claves* del *Suscriptor,* la FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares*, que son generadas bajo el exclusivo control del *Suscriptor*.

6.1.2. Envío de la clave privada al suscriptor

220. No existe ninguna entrega de *Clave privada* en la emisión de los *Certificados* expedidos bajo las presentes *Políticas y Prácticas de Certificación*.

221. En todo caso, si la FNMT-RCM o cualquiera de las oficinas de registro tuviera conocimiento de un acceso no autorizado a la *Clave privada* del *Suscriptor*, el *Certificado* asociado a dicha *Clave privada* será revocado.

6.1.3. Envío de la clave pública al emisor del certificado

222. La *Clave pública,* generada por el *Suscriptor* junto a la *Clave privada* en un dispositivo de generación y custodia de claves, es entregada a la *Autoridad de Certificación* mediante el envío de la solicitud del *Certificado*.

6.1.4. Distribución de la clave pública de la AC a las partes que confían

223. Véase el apartado correspondiente en la DGPC.

6.1.5. Tamaños de claves y algoritmos utilizados

224. El algoritmo utilizado es RSA con SHA-256.

225. En cuanto al tamaño de las claves, dependiendo de cada caso, es:

- Claves de la AC FNMT raíz: 4.096 bits.
- Claves de la AC FNMT Usuarios Subordinada*:* 2.048 bits.
- Claves de los *Certificados de Firma Electrónica:* 2.048 bits.

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

226. Véase el apartado correspondiente en la DGPC.

6.1.7. Usos admitidos de las claves (KeyUsage field X.509v3)

227. Los *Certificados* FNMT incluyen la extensión Key Usage y, según el caso, Extended Key Usage, indicando los usos habilitados de las *Claves*.

228. El *Certificado* de la AC FNMT raíz tiene habilitados los usos de *Claves* para firmar/sellar los *Certificados* de las ACs FNMT Subordinadas y las ARLs.

229. El *Certificado* de la AC FNMT Subordinada que expide los *Certificados de Firma Electrónica* tiene habilitado exclusivamente el uso para firmar/sellar *Certificados* de entidad final y CRLs.

230. Los *Certificados de Firma Electrónica* tienen habilitado exclusivamente los usos de clave de cifrado de claves, autenticación y firma.

6.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE LOS MÓDULOS CRIPTOGRÁFICOS

6.2.1. Estándares para los módulos criptográficos

231. Véase el apartado correspondiente en la DGPC.

6.2.2. Control multi-persona (n de m) de la clave privada

232. Véase el apartado correspondiente en la DGPC.

6.2.3. Custodia de la clave privada

233. Las operaciones de copia, salvaguarda o recuperación de las *Claves privadas* de las *Autoridades de Certificación* de la FNMT-RCM se realizan bajo control exclusivo del personal autorizado, usando, al menos, control dual y en un entorno seguro.

6.2.4. Copia de seguridad de la clave privada

234. Véase el apartado correspondiente en la DGPC.

6.2.5. Archivado de la clave privada

235. Véase el apartado correspondiente en la DGPC.

6.2.6. Trasferencia de la clave privada a o desde el módulo criptográfico

236. Véase el apartado correspondiente en la DGPC.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

237. Véase el apartado correspondiente en la DGPC.

6.2.8. Método de activación de la clave privada

238. Las *Claves privadas* de las *Autoridades de Certificación* son generadas y custodiadas por un dispositivo criptográfico que cumple los requisitos de seguridad FIPS PUB 140-2 Level 3.

239. Los mecanismos de activación y uso de las *Claves privadas* de la *Autoridad de Certificación* se basan en la segmentación de roles de gestión y operación que la FNMT-RCM tiene implementados con mecanismos de acceso multipersona basados en tarjetas criptográficas y sus correspondientes pines en un esquema de uso simultáneo M de N (2 de 5).

6.2.9. Método de desactivación de la clave privada

240. Véase el apartado correspondiente en la DGPC.

6.2.10. Método de destrucción de la clave privada

241. La FNMT-RCM destruirá o almacenará de forma apropiada las Claves del *Prestador de Servicios de Confianza* una vez finalizado el período de validez de las mismas, con la finalidad de evitar su uso inapropiado.

6.2.11. Clasificación de los módulos criptográficos

242. Véase el apartado correspondiente en la DGPC.

6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1. Archivo de la clave pública

243. Véase el apartado correspondiente en la DGPC.

6.3.2. Periodos de operación del certificado y periodos de uso del par de claves

244. Los periodos de operación de los *Certificados* y sus *Claves* asociadas son:

- *Certificado* de la AC FNMT raíz y su par de *Claves*: hasta el 1 de enero de 2030.
- El *Certificado* de la AC subordinada que expide los *Certificados de Firma Electrónica*: hasta el 28 de octubre de 2029.
- Los *Certificados de Firma Electrónica* y su par de *Claves:* no superior a 4 años.

6.4. DATOS DE ACTIVACIÓN

6.4.1. Generación e instalación de datos de activación

245. Los datos de activación, tanto de las *Claves* de la AC FNMT raíz como de las *Claves* de la AC subordinada que expide los *Certificados de Firma Electrónica,* se generan durante la ceremonia de *Claves* de creación de dichas *Autoridades de Certificación*.

6.4.2. Protección de datos de activación

246. Los datos de activación de las *Claves privadas* de la *Autoridad de Certificación* están protegidos, conforme al método descrito en el apartado "6.2.8 Método de activación de la *Clave privada*" del presente documento, con mecanismos de acceso multipersona basados en tarjetas criptográficas y sus correspondientes pines en un esquema de uso simultáneo M de N (2 de 5).

6.4.3. Otros aspectos de los datos de activación

247. No estipulados.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

248. Véase el apartado correspondiente en la *DGPC*.

6.5.1. Requisitos técnicos específicos de seguridad informática

249. Véase el apartado correspondiente en la *DGPC*.

6.5.2. Evaluación del nivel de seguridad informática

250. Véase el apartado correspondiente en la *DGPC*.

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

251. Véase el apartado correspondiente en la *DGPC*.

6.6.1. Controles de desarrollo de sistemas

252. Véase el apartado correspondiente en la *DGPC*.

6.6.2. Controles de gestión de la seguridad

253. Véase el apartado correspondiente en la *DGPC*.

6.6.3. Controles de seguridad del ciclo de vida

254. Véase el apartado correspondiente en la *DGPC*.

6.7. CONTROLES DE SEGURIDAD DE RED

255. Véase el apartado correspondiente en la *DGPC*.

6.8. FUENTE DE TIEMPO

256. Véase el apartado correspondiente en la *DGPC*.

6.9. OTROS CONTROLES ADICIONALES

257. Véase el apartado correspondiente en la *DGPC*.

6.9.1. Control de la capacidad de prestación de los servicios

258. Véase el apartado correspondiente en la *DGPC*.

6.9.2. Control de desarrollo de sistemas y aplicaciones informáticas

259. Véase el apartado correspondiente en la *DGPC*.

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. PERFIL DEL CERTIFICADO

260. Los *Certificados de Firma Electrónica* son expedidos como "cualificados" de conformidad con los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

7.1.1. Número de versión

261. Los *Certificados de Firma Electrónica* son conformes con el estándar X.509 versión 3.

7.1.2. Extensiones del certificado

262. En la página http://www.cert.fnmt.es/dpcs/ se publica el documento que describe el perfil de los *Certificados de Firma Electrónica* emitidos bajo esta política, incluyendo todas sus extensiones.

7.1.3. Identificadores de objeto de algoritmos

263. El identificador de objeto (OID) correspondiente al algoritmo criptográfico utilizado (SHA-256 with RSA Encryption) es 1.2.840.113549.1.1.11

7.1.4. Formatos de nombres

264. La codificación de los *Certificados* sigue la recomendación RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Todos los campos definidos en el perfil de los *Certificados* de las presentes *Políticas de Certificación,* excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

265. En la página http://www.cert.fnmt.es/dpcs/ se publica el documento que describe el perfil de los *Certificados de Firma Electrónica* emitidos bajo esta política, incluyendo todas sus extensiones.

7.1.5. Restricciones de nombres

266. El nombre distintivo (*DN*) asignado al *Sujeto* del *Certificado*, en el ámbito de la presente *DPPP*, será único y con la composición definida en el perfil del *Certificado*.

7.1.6. Identificador de objeto de política de certificado

267. El identificador de objeto (OID) de la política del *Certificado de Firma Electrónica* es la definida en el apartado "1.2 Nombre del documento e identificación" del presente documento.

7.1.7. Empleo de la extensión restricciones de política

268. La extensión Policy Constrains del *Certificado* raíz de la AC no es utilizado.

7.1.8. Sintaxis y semántica de los calificadores de política

269. La extensión Certificate Policies incluye dos campos de Policy Qualifiers:

- CPS Pointer: contiene la URL donde se publica la *DGPC* y las *Políticas de Certificación* y *Prácticas de Certificación Particulares* aplicables a los *Certificados.*
- User notice: contiene un texto que puede ser desplegado en la pantalla del usuario del *Certificado* durante la verificación del mismo.

7.1.9. Tratamiento semántico para la extensión "certificate policy"

270. La extensión Certificate Policy incluye el campo OID de política, que identifica la política asociada al *Certificado* por parte de la FNMT–RCM, así como los dos campos relacionados en el apartado anterior.

7.2. PERFIL DE LA CRL

7.2.1. Número de versión

271. El perfil de las CRL son conformes con el estándar X.509 versión 2.

7.2.2. CRL y extensiones

272. El perfil de las CRL sigue la siguiente estructura:

Tabla 3 – Perfil de la CRL

Campos y extensiones	Valor
Versión	V2

Campos y extensiones	Valor
Algoritmo de firma	Sha256WithRSAEncryption
Número de CRL	Valor incremental
Emisor	DN del emisor
Fecha de emisión	Tiempo UTC de emisión.
Fecha de próxima actualización	Fecha de emisión + 24 horas
Identificador de la clave de Autoridad	Hash de la clave del emisor
ExpiredCertsOnCRL	NotBefore de la CA
Punto de distribución	URLs del punto de distribución y ámbito de las CRLs
Certificados revocados	Lista de certificados revocados, conteniendo al menos para cada entrada, número de serie y fecha de revocación

7.3. PERFIL DE OCSP

7.3.1. Número de versión

273. Véase el apartado correspondiente en la *DGPC*.

7.3.2. Extensiones del OCSP

274. Véase el apartado correspondiente en la *DGPC*.

8. AUDITORÍAS DE CUMPLIMIENTO

275. El sistema de expedición de *Certificados* es sometido anualmente a un proceso de auditoría conforme a los estándares europeos ETSI EN 319 401 "General Policy Requirements for Trust Service Providers" y ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates".

276. Así mismo, los *Certificados* tienen la consideración de cualificados, por lo que la auditoría garantiza el cumplimiento con los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates".

277. El sistema de expedición de *Certificados* es sometido a otras auditorías adicionales:

- Auditoría del Sistema de Gestión de la Seguridad de la Información conforme a UNE-ISO/IEC 27001 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos".
- Auditoría según lo dictaminado en el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica).
- Auditoría del Sistema de Gestión de la Calidad con arreglo a ISO 9001.
- Auditoría del Sistema de Gestión de la Responsabilidad Social en correspondencia con IQNet SR10.
- Auditoría del Plan de continuidad de negocio según ISO 22301.
- Auditoría conforme el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (RGPD / LOPD-GDD).

278. También se llevan a cabo análisis de riesgos, de acuerdo a lo dictado en el Sistema de Gestión de la Seguridad de la Información.

8.1. FRECUENCIA DE LAS AUDITORÍAS

279. Periódicamente se elaborarán los correspondientes planes de auditorías.

280. La *Autoridad de Certificación* que expide los *Certificados de Firma Electrónica* está sujeta a auditorías periódicas, de conformidad con el estándar europeo ETSI EN 319 401 "General Policy Requirements for Trust Service Providers", ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons". La auditoría es realizada anualmente por una empresa externa acreditada.

281. La frecuencia del resto de auditorías adicionales, será conforme a lo estipulado en la normativa vigente correspondiente.

8.2. CUALIFICACIÓN DEL AUDITOR

282. Véase el apartado correspondiente en la *DGPC.*

8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

283. Véase el apartado correspondiente en la *DGPC*.

8.4. ELEMENTOS OBJETOS DE AUDITORÍA

284. Véase el apartado correspondiente en la *DGPC*.

8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

285. Véase el apartado correspondiente en la *DGPC*.

8.6. COMUNICACIÓN DE LOS RESULTADOS

286. Véase el apartado correspondiente en la *DGPC*.

8.7. AUTOEVALUACIÓN

287. Véase el apartado correspondiente en la *DGPC*.

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

288. Véase el apartado correspondiente en la *DGPC*.

9.1.1. Tarifas de emisión o renovación de certificados

289. Véase el apartado correspondiente en la *DGPC*.

9.1.2. Tarifas de acceso a los certificados

290. No estipulado.

9.1.3. Tarifas de acceso a la información de estado o revocación

291. La FNMT-RCM ofrece los servicios de información del estado de los certificados a través de CRL o del OCSP de forma gratuita.

9.1.4. Tarifas para otros servicios

292. Véase el apartado correspondiente en la *DGPC*.

9.1.5. Política de reembolso

293. Los Certificados emitidos bajo esta *DPPP* no conllevan gasto alguno para los *Suscriptores*, por lo que no procede establecer política de reembolso.

9.2. RESPONSABILIDAD FINANCIERA

294. Véase el apartado correspondiente en la *DGPC*.

9.2.1. Seguro de responsabilidad civil

295. Véase el apartado correspondiente en la DGPC.

9.2.2. Otros activos

296. Véase el apartado correspondiente en la DGPC.

9.2.3. Seguros y garantías para entidades finales

297. Véase el apartado correspondiente en la DGPC.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

298. Véase el apartado correspondiente en la *DGPC*.

9.3.1. Alcance de la información confidencial

299. Véase el apartado correspondiente en la DGPC.

9.3.2. Información no incluida en el alcance

300. Véase el apartado correspondiente en la DGPC.

9.3.3. Responsabilidad para proteger la información confidencial

301. Véase el apartado correspondiente en la DGPC.

9.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

302. Véase el apartado correspondiente en la *DGPC*.

9.4.1. Plan de privacidad

303. Véase el apartado correspondiente en la DGPC.

9.4.2. Información tratada como privada

304. Véase el apartado correspondiente en la DGPC.

9.4.3. Información no considerada privada

305. Véase el apartado correspondiente en la DGPC.

9.4.4. Responsabilidad de proteger la información privada

306. Véase el apartado correspondiente en la DGPC.

9.4.5. Aviso y consentimiento para usar información privada

307. Véase el apartado correspondiente en la DGPC.

9.4.6. Divulgación conforme al proceso judicial o administrativo

308. Véase el apartado correspondiente en la DGPC.

9.4.7. Otras circunstancias de divulgación de información

309. Véase el apartado correspondiente en la DGPC.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

310. Véase el apartado correspondiente en la *DGPC*.

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. Obligaciones de la AC

311. Las obligaciones y responsabilidades de la FNMT-RCM, como *Prestador de Servicios de Confianza*, con el *Titular* del *Certificado de Persona Física* y el resto de miembros de la Comunidad Electrónica, quedarán determinadas principalmente, por el documento relativo a las condiciones de utilización o el contrato de expedición del *Certificado*, y, subsidiariamente, por las presentes Políticas y Prácticas de Certificación Particulares y por la *DGPC*.

312. La FNMT – RCM cumple los requisitos de las especificaciones técnicas de la norma ETSI EN 319 411 para la emisión de *Certificados* cualificados y se compromete a continuar cumpliendo con dicha norma o aquellas que la sustituyan.

313. Véase el apartado correspondiente en la *DGPC*.

9.6.2. Obligaciones de la AR

314. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, las *Oficinas de Registro* tienen la obligación de:

i) Comprobar fehacientemente la identidad y cualesquiera circunstancias personales de los *Solicitantes* de los *Certificados* relevantes para el fin propio de estos, utilizando cualquiera de los medios admitidos en Derecho, y conforme a lo previsto en la *DGPC* y con carácter particular en la presente *Declaración de Prácticas de Certificación Particulares*.

ii) Conservar toda la información y documentación relativa a los *Certificados de Persona física*, cuya solicitud, renovación o revocación gestiona durante el plazo de tiempo establecido en la legislación vigente.

iii) Permitir a la FNMT-RCM el acceso a los archivos y la auditoría de sus procedimientos en relación con los datos obtenidos en calidad de *Oficina de Registro*.

iv) Informar a la FNMT-RCM de cualquier aspecto que afecte a los *Certificados* expedidos por dicha Entidad (ej.: solicitudes de expedición, renovación…).

v) Comunicar a la FNMT-RCM de forma diligente las solicitudes de expedición de *Certificados*.

vi) Respecto de la extinción de la validez de los *Certificados:*

1. Comprobar diligentemente las causas de revocación que pudieran afectar a la vigencia de los *Certificados*.

2. Comunicar a la FNMT-RCM de forma diligente las solicitudes de revocación de los *Certificados*.

vii) Respecto de la Protección de Datos de Carácter Personal, será de aplicación lo dispuesto en el apartado correspondiente de la *DGPC.*

viii) Las Oficinas de Registro, a través del personal adscrito al servicio por relación laboral o funcionarial, deberán ejercer funciones públicas de acuerdo con la legislación específica aplicable a la FNMT-RCM.

315. En todo caso la FNMT-RCM podrá repetir contra la Oficina de Registro que hubiera realizado el procedimiento de identificación, iniciando las acciones correspondientes, si la causa del daño tuviera su origen en la actuación dolosa o culposa de ésta.

316. Véase el apartado correspondiente en la *DGPC*.

9.6.3. Obligaciones del suscriptor

9.6.3.1. Responsabilidad del Solicitante

317. El *Solicitante* responderá de que la información presentada durante la solicitud del *Certificado* es verdadera y que la solicitud y descarga del *Certificado* se realizan desde un equipo o dispositivo que puede utilizar, con un alto nivel de confianza, bajo su control exclusivo.

318. El *Solicitante* mantendrá a salvo y defenderá a su costa a la FNMT-RCM contra cualquier acción que pudiese emprenderse contra esta Entidad como consecuencia de la falsedad de la información suministrada en el mencionado procedimiento de expedición del *Certificado*, o contra cualquier daño y perjuicio que sufra la FNMT-RCM como consecuencia de un acto u omisión del *Solicitante*.

9.6.3.2. Responsabilidad del Suscriptor

319. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *DGPC*, el *Titular* del *Certificado de Persona Física*, como *Suscriptor* del *Certificado* y sus *Claves*, tiene la obligación de:

- Custodiar adecuadamente el *Certificado*, los *Datos de Creación de Firma* y, en su caso, la tarjeta o soporte del *Certificado,* poniendo los medios necesarios para impedir su utilización por personas distintas a su *Titular*.
- No utilizar el *Certificado* cuando alguno de los datos incluidos en el *Certificado* sea inexacto o incorrecto, o existan razones de seguridad que así lo aconsejen.
- Comunicar a la FNMT-RCM la pérdida, extravío o sospecha de ello, del *Certificado,* de los *Datos de Creación de Firma,* de la tarjeta o soporte del *Certificado* del que es *Titular*, con el fin de iniciar, en su caso, los trámites de su revocación.

320. Será responsabilidad del *Titular* informar a la FNMT-RCM acerca de cualquier variación de estado o información respecto de lo reflejado en el *Certificado*, para su revocación y nueva expedición.

321. Asimismo, será el *Titular* quien deba responder ante los miembros de la *Comunidad electrónica* y demás *Entidades usuarias* o, en su caso, ante terceros del uso indebido del *Certificado*, o de la falsedad de las manifestaciones en él recogidas, o actos u omisiones que provoquen daños y perjuicios a la FNMT-RCM o a terceros.

322. Será responsabilidad y, por tanto, obligación del *Titular* no usar el *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado en la actividad como Entidad emisora de *Certificados* y no se hubiera producido la subrogación prevista en la ley. En todo caso, el *Titular* no usará el *Certificado* en los casos en los que los *Datos de Creación de Firma / Sello* del *Prestador* puedan estar amenazados y/o comprometidos, y así se haya comunicado por el *Prestador* o, en su caso, el *Titular* hubiera tenido noticia de estas circunstancias.

9.6.4. Obligaciones de las partes que confían

323. Véase el apartado correspondiente en la *DGPC*.

9.6.5. Obligaciones de otros participantes

324. No estipulado.

9.7. RENUNCIA DE GARANTÍAS

325. No estipulado.

9.8. LIMITACIONES DE RESPONSABILIDAD

326. Véase el apartado correspondiente en la *DGPC*.

9.9. INDEMNIZACIONES

327. Véase el apartado correspondiente en la *DGPC*.

9.9.1. Indemnización de la CA

328. No estipulado.

9.9.2. Indemnización de los Suscriptores

329. No estipulado.

9.9.3. Indemnización de las partes que confían

330. No estipulado.

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

331. La presente *Declaración de Prácticas y Políticas de Certificación* entrará en vigor en el momento de su publicación.

9.10.2. Terminación

332. La presente *Declaración de Prácticas y Políticas de Certificación* será derogada en el momento que una nueva versión del documento sea publicada. La nueva versión sustituirá íntegramente al documento anterior. La FNMT – RCM se compromete a someter dicha Declaración a un proceso de revisión anual.

9.10.3. Efectos de la finalización

333. Para los *Certificados* vigentes emitidos bajo una *Declaración de Prácticas y Políticas de Certificación* anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

334. Véase el apartado correspondiente en la *DGPC*.

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. Procedimiento para las modificaciones

335. Véase el apartado correspondiente en la *DGPC*.

9.12.2. Periodo y mecanismo de notificación

336. Véase el apartado correspondiente en la *DGPC*.

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

337. Véase el apartado correspondiente en la *DGPC*.

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

338. Véase el apartado correspondiente en la *DGPC*.

9.14. NORMATIVA DE APLICACIÓN

339. Véase el apartado correspondiente en la *DGPC*.

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

340. La FNMT-RCM manifiesta el cumplimiento de la normativa de aplicación.

9.16. ESTIPULACIONES DIVERSAS

341. Véase el apartado correspondiente en la *DGPC*.

9.16.1. Acuerdo íntegro

342. Véase el apartado correspondiente en la *DGPC*.

9.16.2. Asignación

343. Véase el apartado correspondiente en la *DGPC*.

9.16.3. Severabilidad

344. Véase el apartado correspondiente en la *DGPC*.

9.16.4. Cumplimiento

345. Véase el apartado correspondiente en la *DGPC*.

9.16.5. Fuerza Mayor

346. Véase el apartado correspondiente en la *DGPC*.

9.17. OTRAS ESTIPULACIONES

347. No se contemplan.